



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/733,014	12/07/2000	Michael Wray	B-4051 618407-2	2473

7590 06/08/2004

LADAS & PARRY

Suite 2100

5670 Wilshire Boulevard

Los Angeles, CA 90036-5679

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 06/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/733,014

Applicant(s)

WRAY ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 August 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date #6. | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in response to the communication filed on 08/23/2002. Claims 1 – 21 were received for consideration. Preliminary amendments to the claims were filed. Claims 3 and 6 were deleted. Claims 1, 2, 4, 5 and 7 – 21 are currently being considered.
2. An initialed and dated copy of Applicant's IDS form 1449; Paper No.6 is attached to the Office action.

Claim Objections

3. Claims 10, 12, 16 and 18 are objected to because of the following informalities:
Period is missing at the end of each of the claims.
Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section

351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2, 4, 5 and 7 – 21 rejected under 35 U.S.C. 102(e) as being anticipated by Aziz et al. (U.S. Patent No.: 6,643,701)

Regarding Claim 1, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems, the communication means including a transport entity for providing transport services, and a transport-independent, session-level security entity logically positioned above the transport entity and visible to the local application entity, the security entity being operative to set up secure communication sessions with peer security entities in other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65) and comprising:

key-exchange handshake means for conducting a handshake with a said peer security entity associated with a particular remote application entity with which said local application entity wishes to communicate, this handshake involving the exchange of key-related data for use in generating session keys (Column 1 lines 24 – 33 and line 56 – Column 2 line 56); and

secure channel means for enabling messages to be passed between the local application entity and said particular remote application entity with authentication and/or encryption of these messages being effected using the session keys generated from

said key-related data whereby to secure these messages in passages between the cooperating security entities (Column 1 line 64 – Column 2 line 7);

the handshake means including

first means, operative in the course of said handshake, to pass to said peer security entity a first indication indicating the services required by the local application entity, to receive back from said peer security entity a second indication indicating the attributes required of the local application entity by the remote application entity for carrying out said services, and to pass first attribute justifications in the form of one or more certificates, to said peer security entity (Column 1 line 64 – Column 2 line 48), and

security entity a third indication indicating the attributes required of the remote application entity by the local application entity, and to receive second attribute justifications, in the form of one or more certificates, from said peer security entity (Column 1 line 56 – Column 2 line 56).

Regarding Claim 13, Hoskinson teaches and describes, a method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), the handshake further involving

passing from the local security entity to the remote security entity a first indication indicating the services required by the local system, passing from the remote security

entity to the local security entity a second indication indicating the attributes required of the local system by the remote system for carrying out said services, and passing from the local security entity to the remote security entity, first attribute justifications in the form of one or more certificates (Column 1 line 64 – Column 2 line 48), and

passing from the local security entity to the remote security entity a third indication indicating the attributes required of the remote system by the local system (Column 1 line 56 – Column 2 line 48), and

passing from the remote security entity to the local security entity second attribute justifications, in the form of one or more certificates (Column 2 lines 7 – 36).

Regarding Claim 20, Hoskinson teaches and describes, a method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), the handshaking further involving:

the local security entity indicating to the remote security entity the services and attributes required of said remote system by the local system (Column 1 lines 24 – 33; line 56 – Column 2 line 56; and Column 8 lines 6 – 33),

the remote security entity indicating to the local security entity the attributes that the remote system requires of the local system in respect of said services (Column 1 line 56 – Column 2 line 56; and Column 8 lines 6 – 41), and

the exchange of attribute justifications, in the form of certificates, between the security entities (Column 1 line 56 – Column 2 line 56).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein

the security entity is capable of establishing multiple concurrent security sessions with another system over a common transport connection set up by the transport entity (Column 1 line 40 – Column 2 line 67 and Column 6 lines 30 – 58).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), further comprising

attribute justification means for providing from certificates received from the remote system during said handshake that the remote application has the required attributes (Column 2 lines 7 – 48 and Column 7 lines 20 – 64).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein

said local application entity is mediation entity acting on behalf of one or more other application entities (Column 5 line 50 – Column 6 line 58).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein the security entity formats its communications intended for the remote peer security entity in protocol data units (PDUs) that each include:

a session indicator enabling the peer security entity to determine to which security session the PDU relates (Column 8 lines 6 – 38 and line 66 – Column 9 line 5);
and

a message-type field by which the peer security entity can determine whether the PDU carries handshake-related data or a message being passed over the secure channel of the security session indicated by said session indicator (Column 1 line 65 – Column 2 line 67).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein

said handshake is a three message handshake, the first message passing from the local security entity to said peer security entity and including said first and third indications, the second message passing from the peer security entity to the local security entity and including said second indication and said second attribute justifications, and the third message passing from the local security entity to said peer security entity and including said first attribute justifications (Column 1 line 64 – Column 2 line 56).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption algorithms that will be subsequently used by the secure channel means for the security session concerned (Column 1 line 64 – Column 2 line 48).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Hoskinson teaches and describes, a method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein said handshake is a three message handshake, the first message passing from the local security entity to said remote security entity and including said first and third indications, the second message passing from the remote security entity to the local security entity and including said indications and said second attribute justifications, and the third message passing from the local security entity to said third security entity and including said first attribute justifications (Column 1 line 64 – Column 2 line 56).

Claim 15 is rejected as applied above in rejecting claim 13. Furthermore, Hoskinson teaches and describes, a method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption

algorithms to be subsequently used for secure communication between the local and remote systems (Column 1 line 64 – Column 2 line 48).

Claim 19 is rejected as applied above in rejecting claim 13. Furthermore, Hoskinson teaches and describes, a method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein in each security entity formats its communications intended for the remote peer security entity in protocol data units (PDUs) that each include:

- a session indicator enabling the peer security entity to determine to which security session the PDU relates (Column 8 lines 6 – 38 and line 66 – Column 9 line 5);
- and

- a message-type field by which the peer security entity can determine whether the PDU carries handshake-related data or a message being passed over the secure channel of the security session indicated by said session indicator (Column 1 line 65 – Column 2 line 67).

Claim 21 is rejected as applied above in rejecting claim 20. Furthermore, Hoskinson teaches and describes, a method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected

between respective transport independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein said handshake is a three message handshake, comprising:

a first message passing from the local security entity to said remote security entity and indicating the services and attributes required of said remote system by the local system, a second message passing from the remote security entity to the local security entity and indicating the attributes that the remote system requires of the local system in respect of said services, the second message also including attributes justifications provided by the remote system, and a third message passing from the local security entity to said third security entity and including attribute justifications provided by the local system (Column 1 line 64 – Column 2 line 56).

Claim 11 is rejected as applied above in rejecting claim 8. Furthermore, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption algorithms that will be subsequently used by the secure channel means for the security session concerned (Column 1 line 64 – Column 2 line 48).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange (Column 1 line 40 – 55).

Claim 17 is rejected as applied above in rejecting claim 13. Furthermore, Hoskinson teaches and describes, a method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption algorithms to be subsequently used for secure communication between the local and remote systems.

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Hoskinson teaches and describes, a method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport independent, session-level security entities of the local

and remote systems during which handshake key-related data is exchanged for use in generating session keys (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange (Column 1 line 40 – 55).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Hoskinson teaches and describes, a system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange (Column 1 line 40 – 55).

Claim 18 is rejected as applied above in rejecting claim 13. Furthermore, Hoskinson teaches and describes, a method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys (Fig. 9, 10 and Column 1 line 24 – Column 8 line 65), wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange (Column 1 line 40 – 55).

Conclusion

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 or
faxed to: (703) 872-9306 for all formal communications.

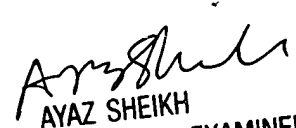
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal
Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Pramila Parthasarathy whose telephone number is 703-
305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for
the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or
proceeding should be directed to the receptionist whose telephone number is 703-305-
3900.

Pramila Parthasarathy
Patent Examiner
703-305-8912
May 28, 2004


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100